REMARKS

This amendment is in response to the Office Action dated November 3, 2006. Reconsideration of the above-identified application in view of the amendments above and the following remarks is respectfully requested.

Claims 1-3, 6, 11, 15, 17, 21-22, 35-36, 59, 62, 71, 74, 80, 108-109, 116-117, 120, 124-125, 152, 157, 166, and 174 are currently pending. Claims 1, 15, 35-36, 59, 71, 74, 80, 108, 117, 120, 124-125, 152 and 166 are hereby amended. Claims 62, 109 and 116 are hereby canceled without prejudice. Claims 180-181 are hereby added.

Claims Objections

In response to the Examiner's objections, the following amendments are hereby made to the claims:

In claim 1, the phrase "digital content" has been restored to the third limitation, as suggested by the Examiner.

In claims 15, 117, 120 and 152 the word "comprise" has been replaced with "comprises".

In claims 35, 36 and 59 the word "input" has been replaced with "input source" and the word "inputs" has been replaced with "input sources".

Claims Rejections under 35 USC 112

In response to the Examiner's rejections under 35 USC 112, the following amendments are hereby made to the claims:

In claim 1, the words "digital media" have been replaced with "digital content".

In claims 59 and 108, the word "relatively" has been deleted.

Claims Rejections under 35 USC 102(e)

Claims 1-3, 6, 11, 15, 17, 21, 22, 35, 36, 59, 108, 109, 166 and 174 are rejected under 35 USC 102(e) as being anticipated over Wang U.S. Patent Number 6,885,748 (hereinafter: Wang).

Unlicensed replication and use of digital content, such as songs, movies and the like, is a prevalent problem today, and results in significant losses to the rightful owners of the content. The present invention significantly increases the difficulty of illegal copying of digital content which has been delivered to an untrusted environment. A first layer of protection is provided by creating a trusted environment within the untrusted environment, which enables the processing of the digital content in such a way that a clear version of the digital content is never available to the user. Additional security is provided by a watchdog component which monitors the integrity of the components which perform the digital content processing, and/or by selecting protective measures for the distributed digital content in accordance with an evaluation of the trustworthiness of the recipient.

In the light of the Examiner's remarks and according to the differences between Wang and the present invention, the Applicant has amended independent claims 1 and 108, emphasizing the distinctiveness of the present invention in the light of the prior art.

Regarding independent claim 1, claim 1 is hereby amended to include producing of trustworthiness credentials regarding the intended recipient environment, and using these trustworthiness credentials to select protective measures for distributing the digital content.

In his comments regarding claim 62, the Examiner states that "Wang fails to teach trustworthiness credentials". Claim 1 therefore clearly includes limitations that are not found in Wang.

Regarding independent claim 108, independent claim 108 is hereby amended to include a watchdog component capable of monitoring at least one digital content handling component.

In his comments to claim 116, the Examiner states that "Wang fails to teach a watchdog component". Amended claim 108 therefore clearly includes limitations that are not found in Wang.

The Applicant therefore believes that amended independent claims 1 and 108 are now novel and inventive over Wang. It is believed that the dependent claims are allowable as being dependent on allowable main claims.

Rejections under 35 USC 103(a)

Claims 62, 71, 74, 80, 116, 117, 120, 124, 125, 152 and 157 are rejected under U.S.C. 103(a) as being unpatentable over Wang in view of Flavin et al. U.S. Patent Number 6,219,788 (hereinafter Flavin).

To establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. In re Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

As discussed above, although Wang relates to using a protective shell to allow the digital content to be decrypted and rendered without ever leaving clear content, Wang lacks both the use of trustworthiness credentials to select protective measures for the content and a watchdog component which monitors the integrity of the processing of the content. The Applicant believes that Flavin neither teaches nor suggests either of these limitations.

Flavin teaches a watchdog system, which serves as "agent trusted by both producers and distributors". Unlike the present invention, the role of Flavin's watchdog is to ensure the "just execution of agreements between a producer of content and a distribution of content" (see Abstract). As such, Flavin's watchdog monitors the operations of the distributor by which the content is transferred from the producer to the subscriber (i.e. content recipient). However, once the content arrives at the subscriber, the distribution is complete and is no longer subject to any agreement between the producer and distributor. Flavin's watchdog therefore does not include any mechanism for evaluating the trustworthiness of the environment which processes the content after delivery, nor does the watchdog perform any monitoring of components involved in such processing.

In order to overcome the rejections of the Examiner, Applicant has chosen to amend independent claim 1 to include the limitation of the production and use of trustworthiness credentials. These trustworthiness credentials provide an evaluation of the *trustworthiness* of the recipient environment, and are used to select security measures for the content being distributed.

> 1. A method for secure distribution of digital content to an untrusted environment of an intended recipient of said digital content, comprising the steps of:

gathering information about said digital content's intended recipient environment;

producing trustworthiness *credentials about said intended recipient environment* based on said information;

selecting protective measures for distributing said digital content in accordance with said trustworthiness credentials;

distributing digital content secured by said selected protective measures to said untrusted environment;

constructing a trusted environment within said untrusted environment;

constructing from said digital content at least two digital input sources, said digital input sources being operable in combination in order to produce a screen rendered version of said digital content;

transferring to said trusted environment such that each of said input sources is transmitted via a different path; and

combining said input sources within said trusted environment in order to produce said screen rendered version of digital content, said trusted environment otherwise preventing access to said digital input sources.

Support is found inter alia in the description of Fig. 4 (para. 220 of the instant specification), which discusses a system for trustworthiness credential assignment, as follows:

> Resulting trustworthiness credentials may be used in order to determine what protective measures should be used, in order to achieve a satisfactory trade-off between ease-of-use and protection level and whether to allow the transaction (in the high risk cases). ...The trustworthiness credential assignment subsystem 440 uses the data from the geo-location data evaluation subsystem 414, the authentication data evaluation subsystem 424, and the components data evaluation subsystem 434 in order to assign trustworthiness credentials to the user. The policy determination subsystem 450 obtains the trustworthiness credentials, and uses them in order to establish a more permissive policy if the user is trustworthy, and a less permissive policy if the user is suspected.

Trustworthiness credentials are based on information gathered about the user's computer environment. The instant specification presents multiple examples of the type of information which is informative about the trustworthiness of the recipient. This information includes geo-location information and the identification of software and hardware components in the user environment that can be used in order to record or copy the data or attempts to tamper with these components.

The Applicant notes that Flavin's distributor does not serve as a recipient environment. The recipient environment, as taught in claim 1, is the environment in which the rendered version is produced. A content distributor does not distribute image data rendered for a display,

due to the large bandwidth which would be required to provide the rendered content to the subscriber. The content distributor is thus unable to serve as a recipient environment.

In Flavin, decisions about the distribution of the content to subscribers are performed by a subscriber selection program. Flavin's subscriber selection program is described in col.7 lines 51-55, which state:

> The decision to distribute content may be based on several inputs. For example, the time and date, expiration of the content and/or subscriber selection programs, and stored records of distribution content.

Subscriber selection may also be based on information fed back from subscriber sites, such as web search information (Flavin col. 8 lines 4-12). The Applicant respectfully submits that none of the information gathered by Flavin provides any information about the trustworthiness of the recipient environment. In consequence, Flavin does not utilize the gathered information to select protective measures for content distribution

Flavin fails to produce or make use of trustworthiness credentials about the intended recipient environment. The trustworthiness of the recipient, or, in other words, the likelihood that the recipient will make illegal use of the content, is not a factor in the distribution decision. The information gathered serves only ensure that the subscriber selection criteria agreed upon by the producer and distributor are adhered to, and, possibly, to format the content as appropriate for the subscriber (for example by embedding advertisements focused at the particular subscriber).

The Applicant therefore believes that claim 1 is inventive over Wang in view of Flavin.

Regarding claim 108, in order to overcome the rejections of the Examiner the Applicant has chosen to amend claim 108 to include the feature of a watchdog component which monitors the digital handling components within the trusted environment. Claim 108 is hereby amended to teach:

> 108. A method for secure distribution of digital content comprising the steps of:
> transferring said digital content to an untrusted environment;
> using a trusted environment within said untrusted environment, said trusted environment being operable to produce a version of said digital content and further being comprised of mechanisms to restrict tampering thereof, wherein said version is rendered for a display,

> said *trusted environment comprising a watchdog component and at least one digital content handling component for producing said version from said digital content, wherein said watchdog component is capable of monitoring at least one of said digital content handling components.*

Support is found inter alia in Fig. 5 and in the accompanying description (para. 222 of the instant specification). Fig. 5 shows a system having a watchdog component 550 and several digital content handling components (e.g. decryption 502 and descrambling and video renderer 560) which are monitored by the watchdog component 550. It is important to note that in the present invention the digital content handling components are those components which transform the distributed content into the rendered version.

In contrast, Flavin provides a watchdog which monitors the producer-distributor-recipient distribution pathway. Flavin's watchdog does not monitor any component which processes the content after distribution. As stated in Flavin col. 4 lines 18-23:

> A computer watchdog system may be installed at the distributor's site or location. The watchdog will monitor and control *information related to the distribution of content...*

Flavin's watchdog is thus seen to be a monitor for content distribution, but does not monitor digital content processing after delivery.

The applicant therefore respectfully submits that neither Wang nor Flavin includes the limitation of a trusted environment comprising a watchdog component capable of monitoring a digital content handling component.

The Applicant therefore believes that claim 108 is inventive over Wang in view of Flavin.

The applicant believes that Wang in view of Flavin does not make obvious all limitations of the amended independent claims 1 and 108. Thus, the Applicant asserts that amended independent claims 1 and 108 are now allowable, and that the dependent claims are consequently allowable as being dependent on allowable main claims.

New Claims

New claims 180-181 are hereby added.

Claims 180 and 181 teach that the trustworthiness credentials comprise geo-location information and geo-location authentication level information respectively. Claim 180 reinstates originally filed claim 68. Claim 181 reinstates originally filed claim 69.

It is believed that all of the matters raised by the Examiner are overcome, and that all of the claims are both novel and inventive. In view of the foregoing, it is submitted that all the claims now pending in the application are allowable over the cited reference. An early Notice of Allowance is therefore respectfully requested.

Respectfully submitted,

Martin D. Moynihan

Martin D. Moynihan
Registration Number 40,338

Date: April 2, 2007

Encl:
Petition for Extension of Two (2) months time
Additional Claims Transmittal